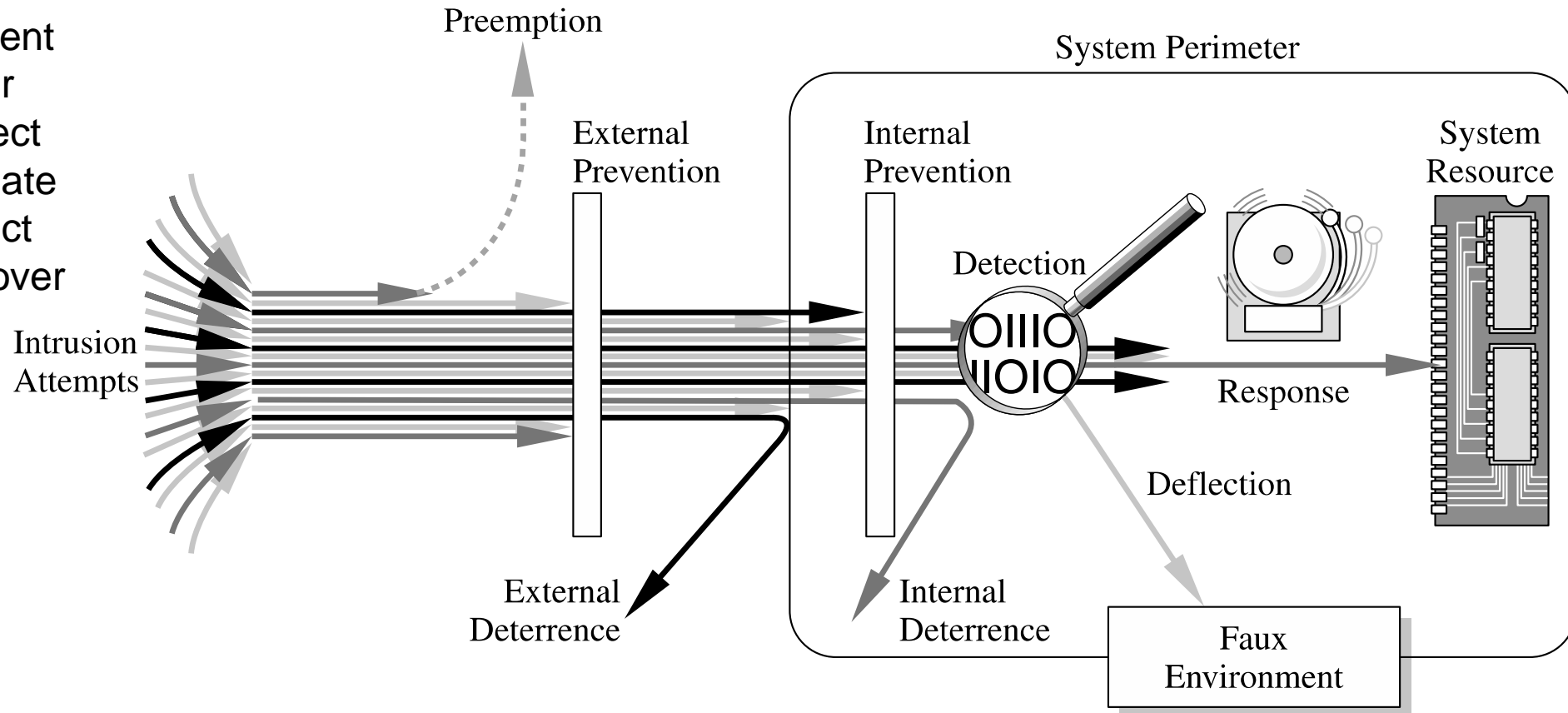


# Apply different types of controls

- Prevent
- Deter
- Deflect
- Mitigate
- Detect
- Recover





# Questions

- Can you give some concrete examples about **control mechanisms**?



# Security by obscurity?

- Obscurity
  - The state of being unknown, inconspicuous, or unimportant.
  - “The system is secure because the attacker won't know X about the system.”
- Obscurity as a security measure
  - E.g., using proprietary crypto mechanisms
- NIST: “system security should not depend on the secrecy of the implementation or its components”
- Better approach: security by design and open security

# Security versus privacy

- Privacy is often defined as having the ability to protect sensitive information about personally identifiable information.
- Others define it as the right to be left alone.
- Achieving security sometimes **sacrifice** privacy.





# Summary

- When we talk about system security, what are we really talking about?
  - Protection of assets of computer system
  - Vulnerability–Threat–Control Paradigm
  - C-I-A triad: confidentiality, integrity, availability
- Think like an attacker when building secured system



# Slides credit

- CS4264: Principles of Computer Security, Gang Wang
- Security in computing 5<sup>th</sup> edition, Textbook Slides



# Authentication

EECS 195

Spring 2019

Zhou Li





# Why need authentication?



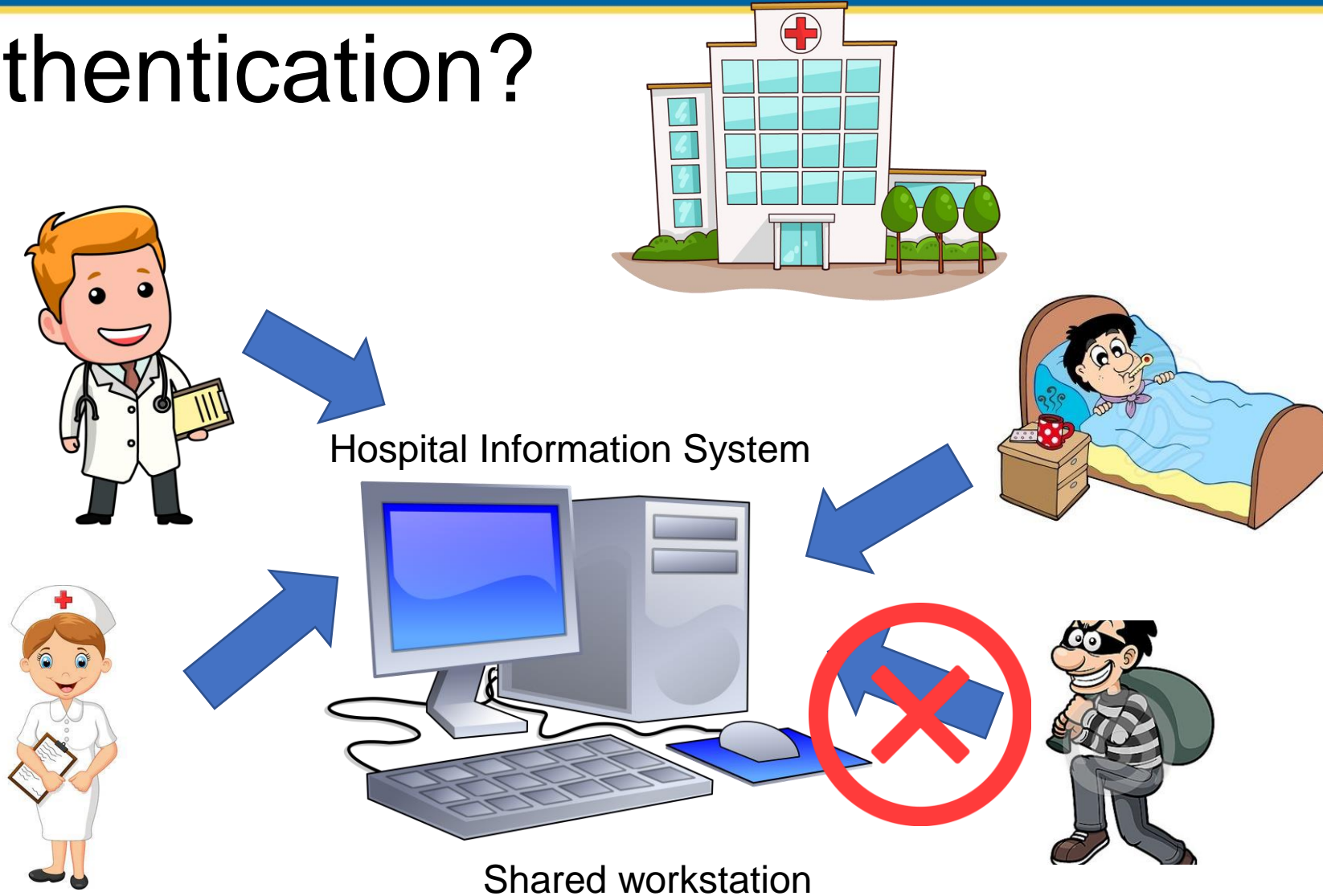
Leo, doctor

Can you build a  
software managing  
medical records?

Sure!



Jim, programmer







# Authentication

- The act of **proving** that a user is who he/she says he/she is
- Methods:
  - Something the user *knows*
  - Something the user *is*
  - Something user *has*
- Identification
  - **Asserting** who a person is
  - Often public/well known
  - Authentication should be private



# Something You Know

- Passwords
- Security questions
- Attacks on “something you know”:
  - Dictionary attacks
  - Password inference
  - Rainbow tables
  - Public information



# Passwords

- Pros
  - Familiar to people, you can have many different ones, easy to revoke / replace, easy to deploy, low cost, ...
- Cons
  - Hard to remember, can be obtained by attacker





# Password storage

- Store passwords in Database of server
- Don't store plaintext on server
- Use hash, salt and pepper!
- Don't check password at browser, **check it at server!**

Identity	Password
Jane	0x471aa2d2
Pat	0x13b9c32f
Phillip	0x01c142be
Roz	0x13b9c32f
Herman	0x5202aae2
Claire	0x488b8c27

LILY HAY NEWMAN SECURITY 03.21.19 02:16 PM

## FACEBOOK STORED MILLIONS OF PASSWORDS IN PLAINTEXT— CHANGE YOURS NOW

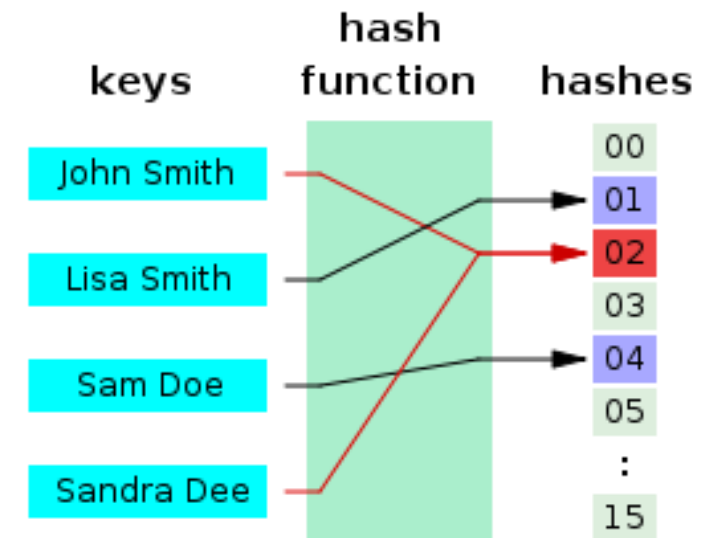
Facebook still got wrong with password storage

<https://www.wired.com/story/facebook-passwords-plaintext-change-yours/>



# Hash function

- Any function **H** that can be used to map data of arbitrary size onto data of a fixed size
- **Cryptographic hash function**
  - **One-way hash function**
    - “Infeasible” to reverse from hash value
    - “Infeasible” to find two messages with same hash
    - Small change of message => big change of hash
- Choose **slow hash function** for password hashing (e.g., **bcrypt**)



A simple hash function



# Salt and pepper

- Salt
  - Random string as additional input to hash function
  - Hash(password||salt)
  - Different password has different salt, stored together with password hash
- Pepper
  - Secret value, not stored in DB
  - Hash(password||salt||pepper)
  - Generated for each application, usually in application code

Username	Salt value	String to be hashed	Hashed value = SHA256 (Salt value + Password)
user1	E1F53135E559C253	password123E1F53135E559C253	72AE25495A7981C40622D49F9A52E4F1565C90F048F59027BD9C8C8900D5C3D8
user2	84B03D034B409D4E	password12384B03D034B409D4E	B4B6603ABC670967E99C7E7F1389E40CD16E78AD38EB1468EC2AA1E62B8BED3A

Not in DB

Password stored with Hash and Salt (Pepper can be appended after Salt)



# Attack passwords - dictionary attack

- Use a program to try a list of words on **target interface (online)** or **password dump (offline)**.
- Online cracking
  - Submit password plaintext to interface
- Offline cracking
  - Compute hash value from plaintext and match
  - Tools are available ([John the Ripper](#), [L0phtCrack](#), and [Cain And Abel](#))

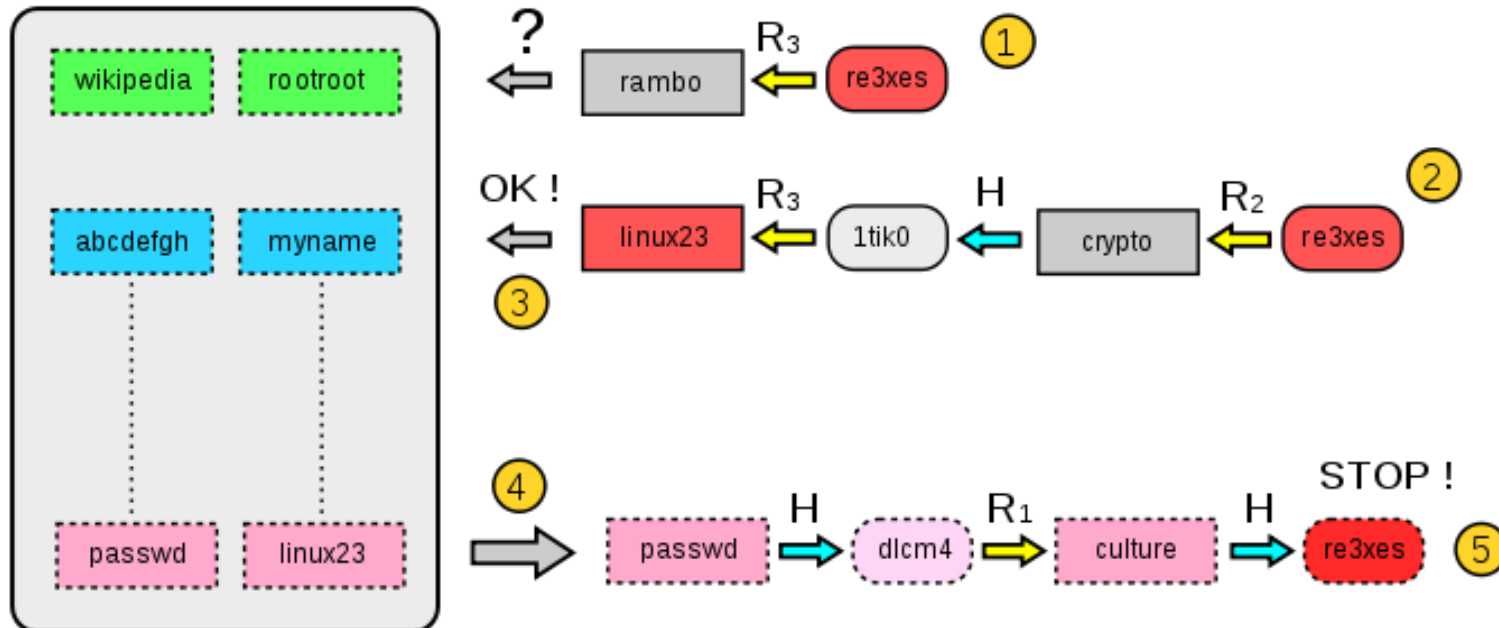




# Attack passwords – rainbow table

- Reuse computed password hash?
- Store all cracked password hash is very **storage-consuming**
- Precomputed **hash chains** to reduce storage

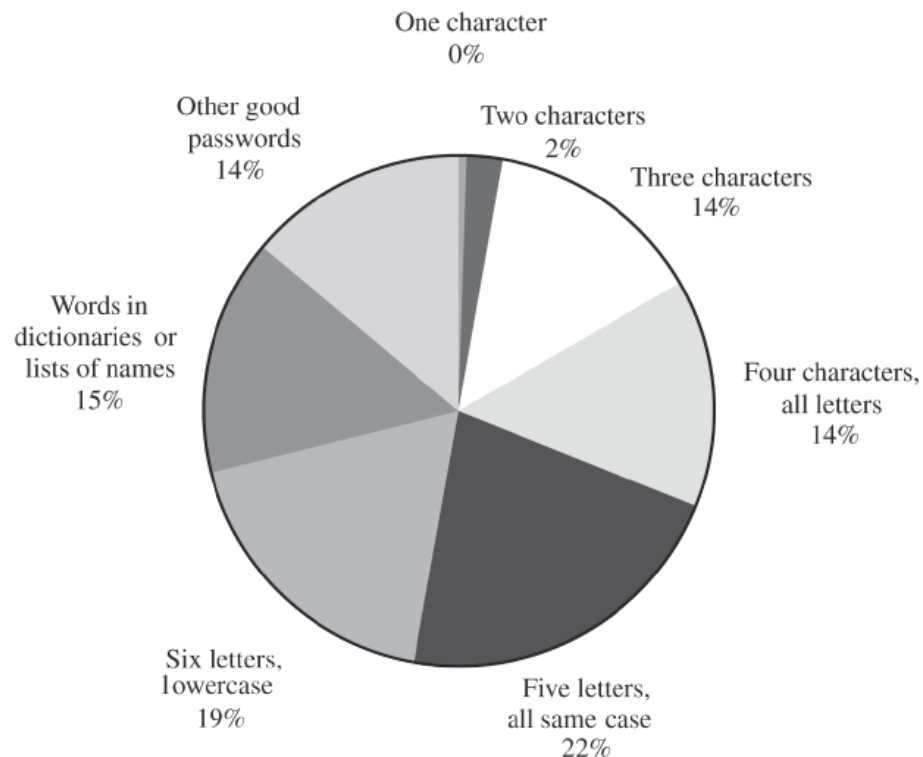
Chain Start Chain End





# Attack passwords - password inference

- Users' password choices are not uniformly distributed



Distribution of 3,289 passwords

## Password leaks

Site	#users	#pass	$\frac{\#pass}{\#users}$
hotmail	7300	6670	0.91
flirtlife	98930	43936	0.44
computerbits	1795	1656	0.92
rockyou	32603043	14344386	0.44

Rank	hotmail	#users	flirtlife	#users	computerbits	#users	rockyou	#users
1	123456	48	123456	1432	password	20	123456	290729
2	123456789	15	ficken	407	computerbits	10	12345	79076
3	111111	10	12345	365	123456	7	123456789	76789
4	12345678	9	hallo	348	dublin	6	password	59462
5	tequiere	8	123456789	258	letmein	5	iloveyou	49952
6	000000	7	schatz	230	qwerty	4	princess	33291
7	alejandro	7	12345678	223	ireland	4	1234567	21725
8	sebastian	6	daniel	185	1234567	3	rockyou	20901
9	estrella	6	1234	175	liverpool	3	12345678	20553
10	1234567	6	askim	171	munster	3	abc123	16648

Investigating the Distribution of Password Choices <https://arxiv.org/pdf/1104.3722.pdf>



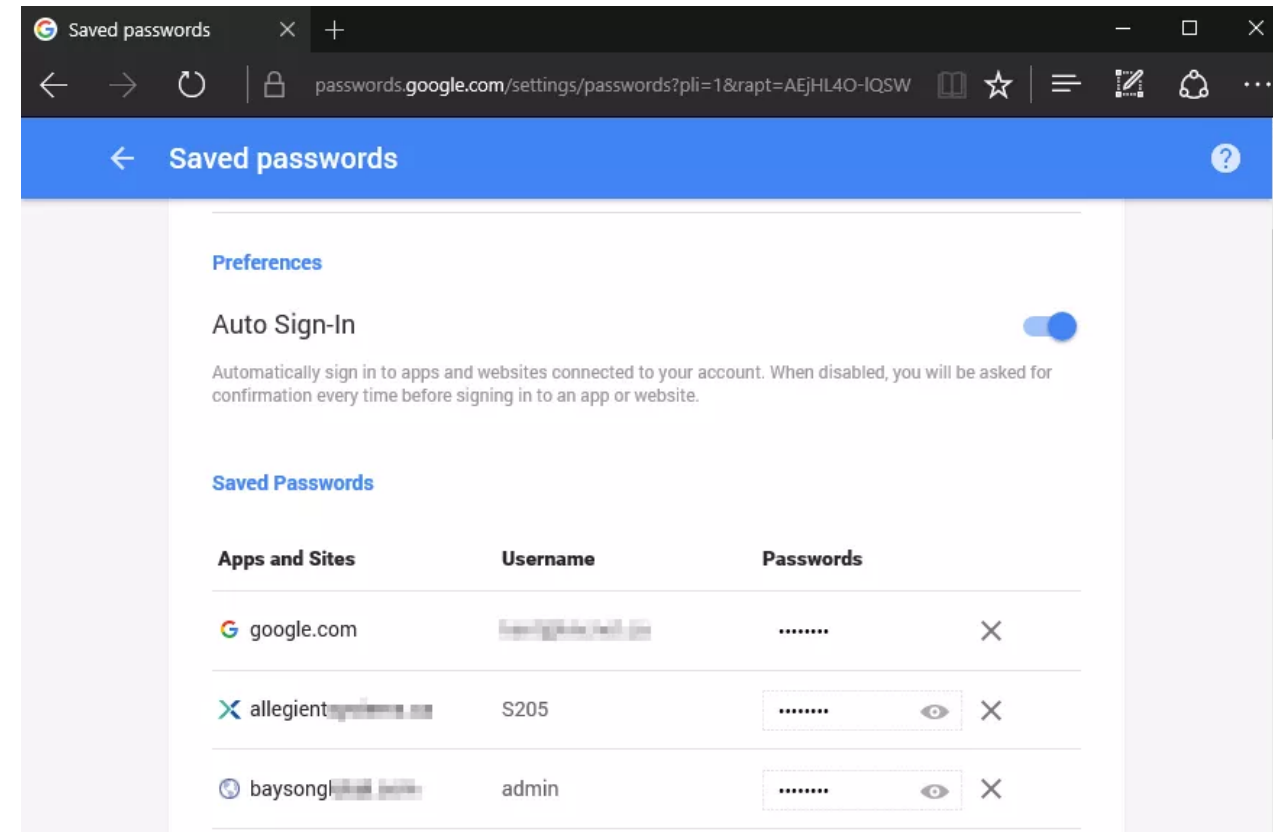
# Question

- What a good password should look like?
  - Use characters other than a-z
  - Choose long passwords
  - ~~• Use a string you can remember~~
  - ~~• Use variants for multiple passwords (based on patterns you remember)~~



# How to manage passwords?


- Don't reuse the same passwords across sites
- Don't write it down on papers or plaintext file
- Password manager is recommended





# Security questions

- Questions to which (presumably) only the right person would know the answer.
- Used a lot for password resetting
- Weakness: can be learnt from public information



**PICK YOUR SECRET QUESTIONS**  
Give yourself another way to recover your account securely in case your information becomes outdated.

**Question 1:**

City where you met your other half? ▾

Answer

**Question 2:**

Name of your favourite band or singer? ▾

Answer

**Question 3:**

Choose your own phrase (at least 2 words) ▾

Answer

**Confirm**

[Cancel](#)



# Attack security questions

- Sarah Palin email hack
- Guy wants to mess with Sarah Palin's campaign
- Try to log in to her Yahoo Mail



David Kernell



# Attack security questions

o!

What did you forget? Verify your identity Reset your password

**What is your alternate email address**  
message with a special link that will let you reset your password.

**For account's alternate email address?**

☐ My alternate email is

☒ I can't access my alternate email address





# Attack security questions

YAHOO! [Yahoo! Home](#) - [Help](#)

Your Progress: [What did you forget?](#) **Verify your identity** [Reset your password](#)

**Answer these questions to validate your identity**  
We need to verify a few questions and we'll be done.

Birthday: February 11 1964

Country of Residence: United States

Postal Code: 99654

[Exit Wizard](#) [Next](#)

Can be found on Wikipedia!



# Attack security questions

The screenshot shows a Yahoo! password reset wizard. At the top left is the Yahoo! logo, and at the top right is a link for "Yahoo! Home - Help". Below the logo is a progress bar with three steps: "What did you forget?", "Verify your identity", and "Reset your password". The "Verify your identity" step is currently active. The main heading is "Please answer your secret question" with the subtext "This is it, we're almost done!". The question is "Where did you meet your spouse?" and the answer entered in the text box is "Wasilla High". A blue arrow points from the text "Her unofficial biography circulating during the campaign" to the answer "Wasilla High". At the bottom left is a link for "Exit Wizard", and at the bottom right is a "Next" button.

YAHOO!

[Yahoo! Home - Help](#)

Your Progress

What did you forget? Verify your identity Reset your password

**Please answer your secret question**  
This is it, we're almost done!

Where did you meet your spouse? Wasilla High

[Exit Wizard](#) [Next](#)

Her unofficial biography circulating during the campaign



# Attack security questions

**YAHOO!** [Yahoo! Home](#) - [Help](#)

Your Progress: **What did you forget?** > **Verify your identity** > **Reset your password**

**Welcome back, Sarah**  
You've verified your account details and may now change your password.

**New Password**

**Re-type New Password**

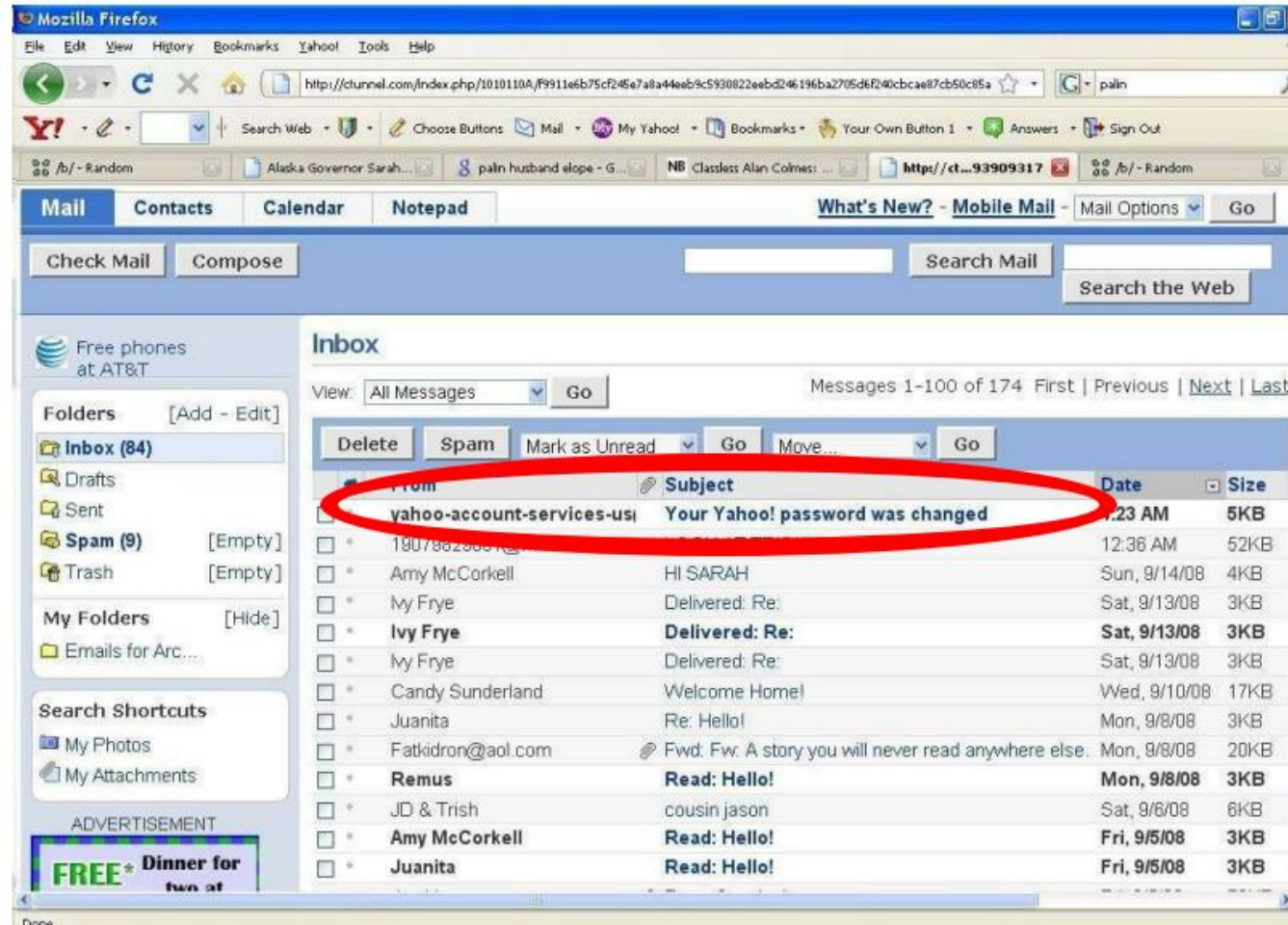
**Password Strength**  
□ □ □ □ □

Changed to "popcorn"

**Next**



# Attack security questions





# Attack security questions

- Consequence: Sentenced to 1 year in federal prison

Lesson: your system is only as secure as the weakest link.







# Aftermath

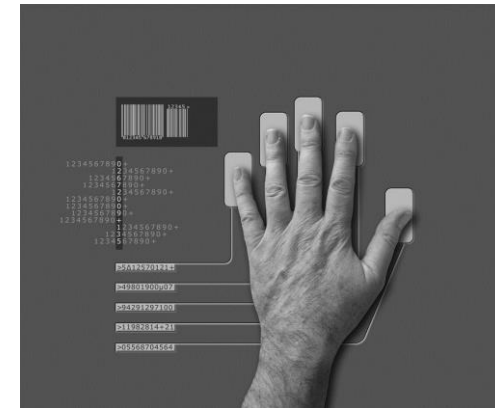
- In 2012, someone hacked Mitt Romney's email account
- ... by guessing the name of his pet dog

Lesson: old attacks remain relevant



# Something you are - biometrics

- **Biometrics** are biological properties, based on some physical characteristic of the human body.
  - fingerprint
  - hand geometry (shape and size of fingers)
  - retina and iris (parts of the eye)
  - voice
  - handwriting, signature, hand motion
  - typing characteristics
  - blood vessels in the finger or hand
  - face
  - facial features, such as nose shape or eye spacing







# Example

Pros/cons?

